IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case no. 6:21-cr-03016-BCW-1
	)	
PATRICIA ASHTON DERGES,	)	
	)	
Defendant.	)	

DEFENDANT'S MOTION TO COMPEL GOVERNMENT REMEDIATION AND CESSATION OF PUBLICATION OF ERRONEOUSLY AND UNLAWFULLY MARKED INDICTMENT AND SUPERSEDING INDICTMENT AS CLASSIFIED

COMES NOW Defendant, Patricia Derges, by and through her counsel, and for Defendant's Motion to Compel Government Remediation and Cessation of Publication of Erroneously and Unlawfully Marked Indictment and Superseding Indictment as Classified, states to the Court as follows:

1. The undersigned counsel recently was engaged to represent the Defendant herein.

2. The present motion has only been filed after a protracted and good faith attempt with the Government to resolve the issues underlying and giving rise to the present motion.

3. The original Indictment herein was marked by the Government as "SECRET."

4. The original Indictment herein, marked "SECRET" was presented to the public at a widely attended and subsequently reported press conference conducted by the Government.

5. The original Indictment herein, marked "SECRET" was thereafter published on the Government's website in PDF form.

6. The Superseding Indictment herein was also marked by the Government as "SECRET."

7. At the time of the unsealing of the Superseding Indictment, while in Court with AUSA Kempf, counsel for Defendant raised concerns about the marking and publishing of the charging documents as "SECRET" and that the misrepresentation by the Government of the charging documents as classified improperly and unfairly cast the Defendant in an unfavorable light in the eyes of the public.

8. This issue was raised with the Court during the Arraignment of the Defendant on the charges set forth in the Superseding Indictment. In keeping with the noting by the Court of the Local Rule requiring good faith efforts to resolve the issue as a condition precedent to raising of same with the Court, the issue was briefly against discussed in the courthouse by counsel for Defendant with AUSA Kempf following the Arraignment of the Defendant on the charges set forth in the Superseding Indictment.

9. As part of this continuing good faith effort to resolve matters with the Government, Defendant's counsel and AUSA Kempf, and subsequently AUSA Kempf's supervisor, AUSA Eggert, exchanged e-correspondence in which Defendant's counsel went to painstaking efforts to explain the issue, the damage unfairly inuring to the detriment of the Defendant as a result of the misclassification of the charging documents, and the law associated therewith.

10. A true and correct copy of the e-correspondence exchanged by and between the Defendant's counsel and the Government's AUSAs is attached hereto, incorporated herein by reference and marked Exhibit A.

11. The term "SECRET", when affixed to a Government document, is indicia of official classification of that document. With the stamp of "SECRET" there are necessarily lawful implications.

12. One of the implications which naturally arises out of the classification by the Government of a charging document is that the charging document contains allegations of misconduct requiring disclosures of some thing or fact which meet the conditions required by the Government to cause said document to be deemed classified.

13. Classification law exists in statutes, executive orders and agency regulations. The Supreme Court in *United States v. Nixon* acknowledged in dicta, and Justice Department policy has asserted, that some national security information is also entitled to be withheld from disclosure as subject to executive privilege under Article II of the Constitution.

14. Various statutes define "classified information" for particular statutory purposes. Congress has only occasionally stepped into classification policy in specific areas, including criminalizing disclosures of classified information under the Espionage Act, or regulating the disclosure of certain intelligence personnel under the Intelligence Identities Protection Act. At least since President Franklin Roosevelt issued Executive Order 8381 in 1940, classification law has been defined primarily by a series of about 20 successive executive orders. (Indeed, the 1995 Intelligence Authorization Act codified what by that year was a half-century-old practice of presidents' defining the procedures for controlling national security information.) Executive Order 13526, the most recent executive order on classification, was issued by President Obama on Dec. 29, 2009, and revoked prior classification orders.

15. Intelligence agencies and other executive branch departments establish regulations that create department-specific policies on classification. For example, Intelligence Community Directive 703 provides guidance on the dissemination of "sensitive compartmented

information" (SCI), a subset of classified information "concerning or derived from intelligence sources, methods or analytical processes." Other agency regulations specifically implement the terms of Executive Order 13526 for that department's needs. For instance, the State Department's Foreign Affairs Manual section on classification provides extensive internal guidance on the handling of "foreign government information," or information provided to the U.S. by foreign governments. Agency regulations also commonly designate internal policy governing which officials may classify or declassify information.

16. Executive Order 13526 specifies that information can be classified through two procedures. First, when information has not been classified before, it may be *originally classified* if it is related to a topic amenable to classification; the information's release would, at a minimum, pose a danger to national security; and a government official with original classification authority—that is, the power to say that a piece of information is classified on first review—designates the information as such. Second, information may be *derivatively classified* if it uses otherwise classified information.

17. Information can be classified in the first instance only if it pertains to at least one of seven topics defined by the executive order:

(a) military plans, weapons systems, or operations;

(b) foreign government information [i.e., information received from foreign governments, with an expectation of confidentiality];

(c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the United States, including confidential sources;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities;

(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(h) the development, production, or use of weapons of mass destruction.

18. Within those topics, the government may classify information under one of three levels based on its sensitivity:

(1) ''Top Secret'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave damage to the national security* that the original classification authority is able to identify or describe.

(2) ''Secret'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *serious damage to the national security* that the original classification authority is able to identify or describe.

(3) ''Confidential'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *damage to the national security* that the original classification authority is able to identify or describe. (Emphasis added.)

19. The order also allows the departments of State, Defense, Energy, Homeland Security and Justice, along with the Office of the Director of National Intelligence, to designate "special access programs," subsets of classified information that are more tightly controlled. The most commonly known special access program is that governing access to information derived from or otherwise related to intelligence sources and methods, which the director of national intelligence controls and has designated as SCI under Intelligence Community Directive 703.

The SCI system helps the intelligence community manage access to particular categories of information among people with access to the appropriate level of classification. So a person with a "top secret" security clearance will ordinarily have access only to a subset of "compartments" within the classification level. (The intelligence community uses the same background-check process—the Single Scope Background Investigation—to authorize employees or contractors to receive both top secret information and SCI, but despite the common designation of holding a "top secret/SCI" clearance, the two categories are distinct.)

20. The executive order also explicitly prohibits certain inappropriate uses of the classification power. The government may not classify information to "conceal violations of law, inefficiency, or administrative error;" "prevent embarrassment to a person, organization, or agency;" "restrain competition;" or otherwise "prevent or delay the release of information that does not require protection in the interest of the national security." In other words, a reasonable belief that disclosure of information would at least damage national security interests is the only valid reason to classify information.

21. Within those parameters, the executive branch tends to earn deference from courts on its classification judgments. Under the U.S. Court of Appeals for the D.C. Circuit's ruling in *McGehee v. Casey*, in cases challenging classification decisions the government must show with "*reasonable specificity* … a logical connection" (emphasis added) between the classified information and the reason for classification. While *McGehee* admonished courts to "satisfy themselves from the record, *in camera* or otherwise, that the [government] in fact had good reason to classify … the materials at issue" and should not presume regularity without verifying the justification, it then retreated, saying judges "cannot second-guess CIA judgments on matters in which the judiciary lacks the requisite expertise." Despite carving out room for judicial

review, *McGehee* left ample discretion to the intelligence community in classification judgments. That deference is evident in subsequent applications of *McGehee*'s standard.

22. Executive Order 13526 also specifies who may designate information as originally classified. The order specifies that the president, the vice president, "agency heads and officials," and officials to whom those officials formally delegate such authority are original classification authorities, sometimes called OCAs. OCAs have authority to classify information up to a specific level: Some officials have the authority to designate information at the top secret level, like the CIA director or the attorney general, while others, like the commerce secretary, may only designate information as secret. OCAs may typically only classify information within their area of responsibility. Additionally, OCAs may delegate their authority to subordinates, often extensively, with some limits based on the level of classification.

23. When intelligence products use information that is already classified, those products may be derivatively classified. Derivative classification does not need to be approved by an OCA, but agencies must issue guidelines for derivative classification by their employees. Further procedural details on derivative classification can be found in Part II of Executive Order 13526 and implementing agency regulations.

24. Just because there's a valid reason to classify information does not automatically mean it is classified. Classification requires an affirmative decision. While much of the sensitive information the government acquires is classified as soon as it comes into the government's possession, some information may not be formally designated as classified until the agency that controls it receives a request, usually from Congress, to share it. One common example is foreign government information, which may not have been classified by the originating government but should nevertheless be classified because public knowledge of the fact that the material has been shared could itself damage national security. Agencies often have specific procedures,

sometimes requiring involvement at more senior levels of the department, for classifying information after it has received an outside request for it.

25. Access to classified information is controlled through the security clearance system, which is coordinated by national security agencies through a branch of the National Archives called the Information Security Oversight Office. The system dates back to the Truman administration, but the modern system, governed by executive order, requires three criteria for a person to gain a security clearance: approval by the head of an authorized agency (usually through the infamously slow, erratic, and widely disclaimed as "broken" security clearance background-check process); a signed classified information nondisclosure agreement; and a need to know the information. Security clearances correspond to the level of information—confidential, secret or top secret—that a person is allowed to have.

26. The government enforces the classification system through classified information nondisclosure agreements and through several criminal statutes, whose application depends on the type of information, the recipient and other circumstances.

27. An array of statutes prohibits the unauthorized handling or disclosure of classified information, aimed at least in part at deterring leaks by government officials. The Intelligence Identities Protection Act, famously at issue in the leak investigation of former CIA officer Valerie Plame's identity to New York Times columnist Robert Novak, prohibits those with access to the identities of covert government officers from disclosing that information.

28. The 1917 Espionage Act also prohibits disclosure of national defense information or classified information. Codified at 18 U.S.C. § 798, it prohibits knowingly disclosing "to an unauthorized person," publishing, or "us[ing] in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States" a variety of classified information. Prosecutors have used the statute to charge

government employees who gave classified information to the media, including Edward Snowden and Pentagon Papers whistleblower Daniel Ellsberg. A separate provision of the Espionage Act, 18 U.S.C. § 793, prohibits, among other things, gathering information regarding "national defense" without authorization or delivering it to people not approved to have it. Several counts in Chelsea Manning's court-martial charge sheet incorporated this provision, and the Justice Department used it to charge Snowden and Julian Assange. Leaks intended to benefit foreign governments may be prosecuted under 18 U.S.C. § 794, often used to charge government employees who give classified information to adversaries.

29. Other statutes make leaking a crime, too. Leaks of diplomatic correspondence may be charged under 18 U.S.C. § 952. And unlawfully retaining classified information, even without disclosing it, may be charged under 18 U.S.C. § 1924.

30. The classified information nondisclosure agreements, such as Standard Form 312, is also a common tool in enforcing security clearances. Prosecutors often cite the contract, which lists the criminal provisions that create liability for unauthorized disclosures, as evidence of an alleged leaker's criminal intent. But in addition to reminding employees of possible tools for criminal liability, the contract creates independent tools for deterring unauthorized disclosure and enforcing the classification system. First, Clause 5 "assign[s] to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement." The government used the analogous provision in the National Security Agency's classified information nondisclosure agreement, for example, to win a court order seizing the proceeds from Edward Snowden's 2019 memoir.

31. Agency-specific nondisclosure agreements typically impose specific requirements for former clearance holders to submit any writing possibly containing classified information to

the agency for review. (The Supreme Court enforced penalties for failing to comply with prepublication requirements in *Snepp v. United States*, but the modern system is the subject of a challenge by the ACLU and Knight Institute currently on appeal in the U.S. Court of Appeals for the Fourth Circuit.) Finally, nondisclosure agreements (and other agency policies) typically prohibit those who unlawfully disclose classified information from holding security clearances in the future. Though perhaps not intended to deter intentional disclosures, such provisions may be a considerable deterrent against reckless or negligent handling of classified information for those making a career in national security.

32. My designating and publishing the Indictment herein, and the subsequent filing with this Court as a matter of public record (both marked "SECRET"), the Government has, by law and by implication, expressly communicated to the world that the Defendant is accused of misconduct involving compromise reasonably be expected to cause serious damage to the national security and that the above referenced charging documents contain information which satisfy the codified conditions precedent to the Government's classification of same as "SECRET." Necessarily, this means the charging documents, if indeed they contain information of this nature, should NOT have been disclosed to the public.

33. Of course, the charging documents referenced above contain no such information. Necessarily, this means the Defendant is being unfairly and unlawfully cast in the negative light associated with one who is accused of compromising national security.

34. The protracted and respectful efforts of Defendant's counsel to educate the AUSAs involved were to no avail, this despite the provision to the AUSAs involved herein of an Herculean effort to do so.

35. In the process, it was also noted for the Government that the Government has wrongfully included in its published Indictment certain personal identifying information ("PII") of the Defendant. The Government failed to redact the PII despite being requested to do so.

36. There is no lawful basis for the Government to classify the Indictment and the Superseding Indictment as "SECRET."

37. Upon information and belief, neither the Indictment nor the Superseding Indictment are or contain that which is required to be classified "SECRET."

38. Having been duly placed on notice of the erroneous nature of the actions of the Government in this regard, the AUSAs remain recalcitrant, effectively placing the Defendant in legal peril and depriving the right of the Defendant to a fair trial.

39. But for the recalcitrance of the AUSAs involved herein, the preparation and prosecution of this motion would not have been required. As such, the Defendant has been forced and compelled to incur legal fees and expenses required to navigate the good faith effort to resolve protocol, prepare, file and present this motion to the Court.

40. The damage caused by the actions of the Government continue to wrongfully and unfairly inure to the detriment of the Defendant. Thus, time is of the essence.

WHEREFORE, Defendant prays this Honorable Court issue an Order directing and mandating the Government:

A. Immediately replace in the Court record copies of the Indictment and Superseding Indictment that are not marked "SECRET";

B. Immediately cause to cease any further publication, distribution or reference to an Indictment or Superseding Indictment filed herein as "SECRET", including specifically the PDF iteration thereof placed on the Government's Justice website;

C. Issue a release and cause same to be distributed to all to whom the Government has previously issued releases in connection with the present matter confirming that the Indictment and Superseding Indictment were erroneously and wrongfully designated as "SECRET" classified documents and that this error should not be interpreted to cast the Defendant in a negative light;

D. To award the Defendant reasonable legal fees and expenses to justly compensate the Defendant for being compelled to prepare, file, present and argue the present motion;

E. To garner from the Court such Order or directive as is necessary to facilitate the removal from the record herein and the public eye any copies of charging documents marked "SECRET."

F. The redaction by the Government of any and all of Defendant's PII from the revised charging documents to be filed with the Court or otherwise published by the Government.

KODNER WATKINS, LC

By: /s Albert S. Watkins

ALBERT S. WATKINS, LC MO#34553
7733 Forsyth Boulevard, Suite 600
Clayton, Missouri 63105
(314) 727-9111
(314) 727-9110 Facsimile
E-mail: albertswatkins@kwklaw.net

COUNSEL FOR DEFENDANT

CERTIFICATE OF SERVICE

Signature above is also certification that on April 5, 2021 a true and correct copy of the foregoing was electronically filed with the Clerk of the Court utilizing the CM/ECF system which will send notification of such filing to all parties of record.

EXHIBIT A

From: Eggert, Randy (USAMOW) [mailto:Randy.Eggert@usdoj.gov]
Sent: Friday, April 02, 2021 10:50 AM
To: Albert Watkins <al@kwklaw.net>; Kempf, Shannon (USAMOW) <Shannon.Kempf@usdoj.gov>
Cc: Robert Seipp <rseipp@kwklaw.net>; Tony Bretz <tbretz@kwklaw.net>; Aimee Gronborg <agronborg@kwklaw.net>
Subject: RE: USA v. Derges [21-145][AG SF]

Mr. Watkins, I am Shannon Kempf's immediate supervisor, and am also assisting him in this case. I am very much aware of the facts of this case, and have consulted with, and have approved all of, Mr. Kempf's email communications to you. You have made whatever point you are trying to make concerning the "sealed" and "secret" issue that you believe exists concerning the superseding indictment. We disagree with your thoughts on the subject and believe that further e-mail communications on the subject do nothing to resolve the issue that you believe exists. We are ready, and eager, to respond to whatever pretrial motion you may file on the issue and invite you to file such a motion.

Further, the pretrial conference in this case is next week. You have not signed the Government's discovery non-dissemination letter, in order to obtain discovery, nor have you availed yourself to view the discovery in this case in our office as we have offered. You have repeatedly indicated that you refuse to sign the discovery non-dissemination letter, which every other criminal defense attorney practicing in the Western District of Missouri signs in order to receive copies of the discovery. As with the "secret" indictment issue, we urge you to file whatever motion you deem necessary to bring this issue to the Court. We also look forward to responding to this motion.

The trial date in this case is the week of May 3 and the Government is ready to proceed to trial on that date. In compliance with the scheduling order, on Monday the Government will send you a proposed plea offer in the case for your client to consider.

Best Regards,

Randy Eggert
Supervisory Assistant United States Attorney
Western District of Missouri
901 E. St. Louis Street, Suite 500
Springfield, Missouri 64804
(417) 575-8105
E-Mail: randy.eggert@usdoj.gov

From: Albert Watkins <al@kwklaw.net>
Sent: Thursday, April 1, 2021 4:55 AM
To: Kempf, Shannon (USAMOW) <SKempf@usa.doj.gov>
Cc: Eggert, Randy (USAMOW) <REggert@usa.doj.gov>; Robert Seipp <rseipp@kwklaw.net>; Tony Bretz <tbretz@kwklaw.net>; Aimee Gronborg <agronborg@kwklaw.net>
Subject: Re: USA v. Derges [21-145][AG SF]

Dear Mr. Kempf:

I am out of my office at this time. I return to my office next Monday.

I simply want to stress that the term "SECRET" cannot be equated with "SEALED" or "CONFIDENTIAL." They are different...very different.

The Government has the duty to not misclassify released charging documents. It is not the duty of a defendant to do so.

The administration of justice requires the Government adhere to the rules as they relate to the marking of records as classified.

The misclassification of the charging documents in this case (and the publication of same) improperly casts our client in the public eye in an erroneous and negative light.

As an Assistant U.S. Attorney you are the individual responsible for the pleadings and filings made a part of the record made by the Government in this case.

This responsibility is not one which can be disregarded or deflected to others.

My contact in this regard continues out of an overwhelming desire to accord you the opportunity to address and reconcile the continuing issue as it relates to the professional and ethical duties of counsel.

I remain available to take your call if you wish to discuss this further.

Sent from my iPhone

Albert S. Watkins LC
Kodner Watkins, LC
7733 Forsyth Blvd., Suite 600
St. Louis, Missouri 63105
314-727-91111
314-727-9110 Facsimile
albertswatkins@kwklaw.net
www.kwklaw.net

it is transmitted; and, (3) persons not participating in our communication may intercept our communications by improperly accessing either of our computers or another computer unconnected to either of us through which the E-Mail is passed. I am communicating with you by E-Mail at your request and with your consent. In the event you do not wish this form of communication in the future, upon your notification of same, no further E-Mail communication will be forthcoming.

On Mar 30, 2021, at 7:33 PM, Kempf, Shannon (USAMOW) <Shannon.Kempf@usdoj.gov> wrote:

Dear Mr. Watkins:

Thank you for your e-mail this morning. As I wrote in my e-mail of March 29, 2021, if you have any further concerns in this regard, please bring the matter to the attention of the Court in a pretrial motion.

Sincerely,

Shannon Kempf
Assistant United States Attorney
Western District of Missouri

From: Albert Watkins <al@kwklaw.net>
Sent: Tuesday, March 30, 2021 9:16 AM
To: Kempf, Shannon (USAMOW) <SKempf@usa.doj.gov>
Subject: RE: USA v. Derges [21-145][AG SF]

Dear Mr. Kempf:

I write with punctilious respect for brethren counsel.

I am going out of my way be design to put you in a position of knowledge about the seriousness of this issue.

Classification law exists in statutes, executive orders and agency regulations. The Supreme Court in *United States v. Nixon* acknowledged in dicta, and Justice Department policy has asserted, that some national security information is also entitled to be withheld from disclosure as subject to executive privilege under Article II of the Constitution.

Various statutes define "classified information" for particular statutory purposes. Congress has only occasionally stepped into classification policy in specific areas, including criminalizing disclosures of classified information under the Espionage Act, or regulating the disclosure of certain intelligence personnel under the Intelligence Identities Protection Act. At least since President Franklin Roosevelt issued Executive Order 8381 in 1940, classification law has been defined primarily by a series of about 20 successive executive orders. (Indeed, the 1995 Intelligence Authorization Act codified what by that year was a half-century-old practice of presidents' defining the procedures for controlling national security information.) Executive

Order 13526, the most recent executive order on classification, was issued by President Obama on Dec. 29, 2009, and revoked prior classification orders.

Intelligence agencies and other executive branch departments establish regulations that create department-specific policies on classification. For example, Intelligence Community Directive 703 provides guidance on the dissemination of "sensitive compartmented information" (SCI), a subset of classified information "concerning or derived from intelligence sources, methods or analytical processes." Other agency regulations specifically implement the terms of Executive Order 13526 for that department's needs. For instance, the State Department's Foreign Affairs Manual section on classification provides extensive internal guidance on the handling of "foreign government information," or information provided to the U.S. by foreign governments. Agency regulations also commonly designate internal policy governing which officials may classify or declassify information.

2. How is information classified?

Executive Order 13526 specifies that information can be classified through two procedures. First, when information has not been classified before, it may be *originally classified* if it is related to a topic amenable to classification; the information's release would, at a minimum, pose a danger to national security; and a government official with original classification authority—that is, the power to say that a piece of information is classified on first review—designates the information as such. Second, information may be *derivatively classified* if it uses otherwise classified information.

Information can be classified in the first instance only if it pertains to at least one of seven topics defined by the executive order:

(a) military plans, weapons systems, or operations;

(b) foreign government information [i.e., information received from foreign governments, with an expectation of confidentiality];

(c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the United States, including confidential sources;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities;

(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(h) the development, production, or use of weapons of mass destruction.

Within those topics, the government may classify information under one of three levels based on its sensitivity:

(1) ''Top Secret'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave damage to the national security* that the original classification authority is able to identify or describe.

(2) ''Secret'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *serious damage to the national security* that the original classification authority is able to identify or describe.

(3) ''Confidential'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *damage to the national security* that the original classification authority is able to identify or describe. (Emphasis added.)

The order also allows the departments of State, Defense, Energy, Homeland Security and Justice, along with the Office of the Director of National Intelligence, to designate "special access programs," subsets of classified information that are more tightly controlled. The most commonly known special access program is that governing access to information derived from or otherwise related to intelligence sources and methods, which the director of national intelligence controls and has designated as SCI under Intelligence Community Directive 703. The SCI system helps the intelligence community manage access to particular categories of information among people with access to the appropriate level of classification. So a person with a "top secret" security clearance will ordinarily have access only to a subset of "compartments" within the classification level. (The intelligence community uses the same background-check process—the Single Scope Background Investigation—to authorize employees or contractors to receive both top secret information and SCI, but despite the common designation of holding a "top secret/SCI" clearance, the two categories are distinct.)

The executive order also explicitly prohibits certain inappropriate uses of the classification power. The government may not classify information to "conceal violations of law, inefficiency, or administrative error;" "prevent embarrassment to a person, organization, or agency;" "restrain competition;" or otherwise "prevent or delay the release of information that does not require protection in the interest of the national security." In other words, a reasonable belief that disclosure of information would at least damage national security interests is the only valid reason to classify information.

Within those parameters, the executive branch tends to earn deference from courts on its classification judgments. Under the U.S. Court of Appeals for the D.C. Circuit's ruling in *McGehee v. Casey*, in cases challenging classification decisions the government must show with "*reasonable specificity* … a logical connection" (emphasis added) between the classified information and the reason for classification. While *McGehee* admonished courts to "satisfy themselves from the record, *in camera* or otherwise, that the [government] in fact had good reason to classify … the materials at issue" and should not presume regularity without verifying the justification, it then retreated, saying judges "cannot second-guess CIA judgments on matters in which the judiciary lacks the requisite expertise." Despite carving out room for judicial

review, *McGehee* left ample discretion to the intelligence community in classification judgments. That deference is evident in subsequent applications of *McGehee*'s standard.

3. Who decides whether information is classified?

Executive Order 13526 also specifies who may designate information as originally classified. The order specifies that the president, the vice president, "agency heads and officials," and officials to whom those officials formally delegate such authority are original classification authorities, sometimes called OCAs. OCAs have authority to classify information up to a specific level: Some officials have the authority to designate information at the top secret level, like the CIA director or the attorney general, while others, like the commerce secretary, may only designate information as secret. OCAs may typically only classify information within their area of responsibility. Additionally, OCAs may delegate their authority to subordinates, often extensively, with some limits based on the level of classification.

When intelligence products use information that is already classified, those products may be derivatively classified. Derivative classification does not need to be approved by an OCA, but agencies must issue guidelines for derivative classification by their employees. Further procedural details on derivative classification can be found in Part II of Executive Order 13526 and implementing agency regulations.

4. When does information become classified?

Just because there's a valid reason to classify information does not automatically mean it is classified. Classification requires an affirmative decision. While much of the sensitive information the government acquires is classified as soon as it comes into the government's possession, some information may not be formally designated as classified until the agency that controls it receives a request, usually from Congress, to share it. One common example is foreign government information, which may not have been classified by the originating government but should nevertheless be classified because public knowledge of the fact that the material has been shared could itself damage national security. Agencies often have specific procedures, sometimes requiring involvement at more senior levels of the department, for classifying information after it has received an outside request for it.

5. Who can access classified information?

Access to classified information is controlled through the security clearance system, which is coordinated by national security agencies through a branch of the National Archives called the Information Security Oversight Office. The system dates back to the Truman administration, but the modern system, governed by executive order, requires three criteria for a person to gain a security clearance: approval by the head of an authorized agency (usually through the infamously slow, erratic, and widely disclaimed as "broken" security clearance background-check process); a signed classified information nondisclosure agreement; and a need to know the information. Security clearances correspond to the level of information—confidential, secret or top secret—that a person is allowed to have.

6. How does the government enforce the classification system?

The government enforces the classification system through classified information nondisclosure agreements and through several criminal statutes, whose application depends on the type of information, the recipient and other circumstances.

An array of statutes prohibit the unauthorized handling or disclosure of classified information, aimed at least in part at deterring leaks by government officials. The Intelligence Identities Protection Act, famously at issue in the leak investigation of former CIA officer Valerie Plame's identity to New York Times columnist Robert Novak, prohibits those with access to the identities of covert government officers from disclosing that information.

The 1917 Espionage Act also prohibits disclosure of national defense information or classified information. Codified at 18 U.S.C. § 798, it prohibits knowingly disclosing "to an unauthorized person," publishing, or "us[ing] in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States" a variety of classified information. Prosecutors have used the statute to charge government employees who gave classified information to the media, including Edward Snowden and Pentagon Papers whistleblower Daniel Ellsberg. A separate provision of the Espionage Act, 18 U.S.C. § 793, prohibits, among other things, gathering information regarding "national defense" without authorization or delivering it to people not approved to have it. Several counts in Chelsea Manning's court-martial charge sheet incorporated this provision, and the Justice Department used it to charge Snowden and Julian Assange. Leaks intended to benefit foreign governments may be prosecuted under 18 U.S.C. § 794, often used to charge government employees who give classified information to adversaries. (Steve Vladeck has an informative book chapter on the history of prosecutions under the Espionage Act.)

Other statutes make leaking a crime, too. Leaks of diplomatic correspondence may be charged under 18 U.S.C. § 952. And unlawfully retaining classified information, even without disclosing it, may be charged under 18 U.S.C. § 1924.

The classified information nondisclosure agreements, such as Standard Form 312, is also a common tool in enforcing security clearances. Prosecutors often cite the contract, which lists the criminal provisions that create liability for unauthorized disclosures, as evidence of an alleged leaker's criminal intent. But in addition to reminding employees of possible tools for criminal liability, the contract creates independent tools for deterring unauthorized disclosure and enforcing the classification system. First, Clause 5 "assign[s] to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement." The government used the analogous provision in the National Security Agency's classified information nondisclosure agreement, for example, to win a court order seizing the proceeds from Edward Snowden's 2019 memoir.

Agency-specific nondisclosure agreements typically impose specific requirements for former clearance holders to submit any writing possibly containing classified information to the agency for review. (The Supreme Court enforced penalties for failing to comply with prepublication

requirements in *Snepp v. United States*, but the modern system is the subject of a challenge by the ACLU and Knight Institute currently on appeal in the U.S. Court of Appeals for the Fourth Circuit.) Finally, nondisclosure agreements (and other agency policies) typically prohibit those who unlawfully disclose classified information from holding security clearances in the future. Though perhaps not intended to deter intentional disclosures, such provisions may be a considerable deterrent against reckless or negligent handling of classified information for those making a career in national security.

7. How does all this affect Bolton?

The government's lawsuit alleges that Bolton published classified information in his book, especially information about the president's conversations with foreign government leaders, and that he failed to comply with his contractual prepublication requirements. Bolton's opposition brief, by comparison, argues that he submitted his manuscript to review, that National Security Council senior director Ellen Knight orally approved his manuscript for publication after edits in April, and that the National Security Council subsequently refused to formally clear the book for publication and later asserted that it still contained classified information.

Executive Order 12356 provides:

National Security Information

This Order prescribes a uniform system for classifying, declassifying, and safeguarding national security information. It recognizes that it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Information may not be classified under this Order unless its disclosure reasonably could be expected to cause damage to the national security. NOW, by the authority vested in me as President by the Constitution and laws of the United States of America, it is hereby ordered as follows:

Part 1

Original Classification

Section 1.1 Classification Levels.

(a) National security information (hereinafter 'classified information') shall be classified at one of the following three levels: (1) 'Top Secret' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. (2) 'Secret' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. (3) 'Confidential' shall be applied to information, the unauthorized

disclosure of which reasonably could be expected to cause damage to the national security. (b) Except as otherwise provided by statute, no other terms shall be used to identify classified information. (c) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.

Sec. 1.2 Classification Authority.

(a) Top Secret. The authority to classify information originally as Top Secret may be exercised only by:

(1) the President; (2) agency heads and officials designated by the President in the Federal Register; and (3) officials delegated this authority pursuant to Section 1.2(d). (b) Secret. The authority to classify information originally as Secret may be exercised only by: (1) agency heads and officials designated by the President in the Federal Register; (2) officials with original Top Secret classification authority; and (3) officials delegated such authority pursuant to Section 1.2(d). (c) Confidential. The authority to classify information originally as Confidential may be exercised only by: (1) agency heads and officials designated by the President in the Federal Register; (2) officials with original Top Secret or Secret classification authority; and (3) officials delegated such authority pursuant to Section 1.2(d). (d) Delegation of Original Classification Authority. (1) Delegations of original classification authority shall be limited to the minimum required to administer this Order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority. (2) Original Top Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Section 1.2(a)(2); and the senior official designated under Section 5.3(a)(1), [FN1] provided that official has been delegated original Top Secret classification authority by the agency head. (3) Original Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2) and 1.2(b)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a)(1), [FN1] provided that official has been delegated original Secret classification authority by the agency head. (4) Original Confidential classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2), 1.2(b)(1) and 1.2(c)(1); an official with original Top Secret

classification authority; and the senior official designated under Section 5.3(a)(1), [FN1] provided that official has been delegated original classification authority by the agency head. (5) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this Order. It shall identify the official delegated the authority by name or position title. Delegated classification authority includes the authority to classify information at the level granted and lower levels of classification. (e) Exceptional Cases. When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Sec. 1.3 Classification Categories.

(a) Information shall be considered for classification if it concerns: (1) military plans, weapons, or operations; (2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security; (3) foreign government information; (4) intelligence activities (including special activities), or intelligence sources or methods; (5) foreign relations or foreign activities of the United States; (6) scientific, technological, or economic matters relating to the national security; (7) United States Government programs for safeguarding nuclear materials or facilities; (8) cryptology; (9) a confidential source; or (10) other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. Any determination made under this subsection shall be reported promptly to the Director of the Information Security Oversight Office. (b) Information that is determined to concern one or more of the categories in Section 1.3(a) shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security. (c) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source,

or intelligence sources or methods is presumed to cause damage to the national security. (d) Information classified in accordance with Section 1.3 shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

Sec. 1.4 Duration of Classification.

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified. (b) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The agency shall be responsible for notifying holders of the information of such extensions. (c) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of this Order.

Sec. 1.5 Identification and Markings.

(a) At the time of original classification, the following information shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information: (1) one of the three classification levels defined in Section 1.1; (2) the identity of the original classification authority if other than the person whose name appears as the approving or signing official; (3) the agency and office of origin; and (4) the date or event for declassification, or the notation 'Originating Agency's Determination Required.' (b) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. Agency heads may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers. (c) Marking designations implementing the provisions of this Order, including abbreviations, shall conform to the standards prescribed in implementing directives issued by the Information Security Oversight Office. (d) Foreign government information shall either retain its original classification or be assigned a United States classification that shall ensure a degree of protection at least equivalent to that required by the entity that furnished the information. (e) Information assigned a level of classification under predecessor orders shall be considered as

classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in Section 3.1(b).

Sec. 1.6 Limitations on Classification.

(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security. (b) Basic scientific research information not clearly related to the national security may not be classified. (c) The President or an agency head or official designated under Sections 1.2(a)(2), 1.2(b)(1), or 1.2(c)(1) may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably by recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office. (d) Information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.A. 552a), or the mandatory review provisions of this Order (Section 3.4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior agency official designated under Section 5.3(a)(1), [FN1] or an official with original Top Secret classification authority.

Part 2

Derivative Classification

Sec. 2.1 Use of Derivative Classification.

(a) Derivative classification is (1) the determination that information is in substance the same as information currently classified, and (2) the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority. (b) Persons who apply derivative classification markings shall: (1) observe and respect original classification decisions; and (2) carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

Sec. 2.2 Classification Guides.

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. (b) Each guide shall be approved personally and in writing by an official who: (1) has program or supervisory responsibility over the information or is the senior agency official designated under Section 5.3(a)(1); [FN1] and (2) is authorized to classify information originally at the highest level of classification prescribed in the guide. (c) Agency heads may, for good cause, grant and revoke waivers of the requirement to prepare classification guides for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

Part 3

Declassification and Downgrading

Sec. 3.1 Declassification Authority.

(a) Information shall be declassified or downgraded as soon as national security considerations permit. Agencies shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter. Information that continues to meet the classification requirements prescribed by Section 1.3 despite the passage of time will continue to be protected in accordance with this Order. (b) Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either, or officials delegated such authority in writing by the agency head or the senior agency official designated pursuant to Section 5.3(a)(1). [FN1] (c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified, pending a prompt decision on the appeal. (d) The provisions of this Section shall also apply to agencies that, under the terms of this Order, do not have original classification authority, but that had such authority under predecessor orders.

Sec. 3.2 Transferred Information.

(a) In the case of classified information transferred in conjunction with a transfer fo functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for

purposes of this Order. (b) In the case of classified information that is not officially transferred as described in Section 3.2(a), but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this Order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information. (c) Classified information accessioned into the National Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and agency guidelines.

Sec. 3.3 Systematic Review for Declassification.

(a) The Archivist of the United States shall, in accordance with procedures and timeframes prescribed in the Information Security Oversight Office's directives implementing this Order, systematically review for declassification or downgrading (1) classified records accessioned into the National Archives of the United States, and (2) classified presidential papers or records under the Archivist's control. Such information shall be reviewed by the Archivist for declassification or downgrading in accordance with systematic review guidelines that shall be provided by the head of the agency that originated the information, or in the case of foreign government information, by the Director of the Information Security Oversight Office in consultation with interested agency heads. (b) Agency heads may conduct internal systematic review programs for classified information originated by their agencies contained in records determined by the Archivist to be permanently valuable but that have not been accessioned into the National Archives of the United States. (c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

Sec. 3.4. Mandatory Review for Declassification.

(a) Except as provided in Section 3.4(b), all information classified under this Order or predecessor orders shall be subject to a review for declassification by the originating agency, if: (1) the request is made by a United States citizen or permanent resident alien, a federal agency, or a State or local government; and (2) the request describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort. (b) Information originated by a President, the White House

Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempted from the provisions of Section 3.4(a). The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of the Administrator of General Services or the Archivist pursuant to sections 2107, 2107 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. The information shall remain classified pending a prompt decision on the appeal. (c) Agencies conducting a mandatory review for declassification shall declassify information no longer requiring protection under this Order. They shall release this information unless withholding is otherwise authorized under applicable law. (d) Agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They shall also provide a means for administratively appealing a denial of a mandatory review request. (e) The Secretary of Defense shall develop special procedures for the review of cryptologic information, and the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, after consultation with affected agencies. The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States. (f) In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order: (1) An agency shall refuse to confirm or deny the existence or non- existence of requested information whenever the fact of its existence or non-existence is itself classifiable under this Order. (2) When an agency receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral. In cases in which the originating agency determines in writing that a response under Section 3.4(f)(1) is required, the referring agency shall respond to the requester in accordance with that Section.

Part 4

Safeguarding

Sec. 4.1 General Restrictions on Access.

(a) A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes. (b) Control shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons. (c) Classified information shall not be disseminated outside the executive branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the executive branch. (d) Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. For purposes of this Section, the Department of Defense shall be considered one agency.

Sec. 4.2 Special Access Programs.

(a) Agency heads designated pursuant to Section 1.2(a) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or predecessor orders. Such programs may be created or continued only at the written direction of these agency heads. For special access programs pertaining to intelligence activities (including special activities but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. (b) Each agency head shall establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office, consistent with the provisions of Section 5.2(b)(4), shall have non- delegable access to all such accountings.

Sec. 4.3 Access by Historical Researchers and Former Presidential Appointees.

(a) The requirement in Section 4.1(a) that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived as provided in Section 4.3(b) for persons who: (1) are engaged in historical research projects, or (2) previously have occupied policy-making positions to which they were appointed by the President. (b) Waivers under Section 4.3(a) may be granted only if the originating agency: (1) determines in

writing that access is consistent with the interest of national security; (2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this Order; and (3) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.

Part 5

Implementation and Review

Sec. 5.1 Policy Direction.

(a) The National Security Council shall provide overall policy direction for the information security program. (b) The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. The Administrator shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

Sec. 5.2 Information Security Oversight Office.

(a) The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Director shall have the authority to appoint a staff for the Office. (b) The Director shall: (1) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order, which shall be binding on the agencies; (2) oversee agency actions to ensure compliance with this Order and implementing directives; (3) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect pending a prompt decision on the appeal; (4) have the authority to conduct on-site reviews of the information security program of each agency that generates or handles classified information and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If these reports, inspections, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior official designated under Section 5.3(a)(1) [FN1] may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect pending a prompt decision on the appeal; (5) review requests for

original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval; (6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program; (7) have the authority to prescribe, after consultation with affected agencies, standard forms that will promote the implementation of the information security program; (8) report at least annually to the President through the National Security Council on the implementation of this Order; and (9) have the authority to convene and chair interagency meetings to discuss matters pertaining to the information security program.

Sec. 5.3 General Responsibilities.

Agencies that originate or handle classified information shall: (a) designate a senior agency official to direct and administer its information security program, which shall include an active oversight and security education program to ensure effective implementation of this Order; (b) promulgate implementing regulations. Any unclassified regulations that establish agency information security policy shall be published in the Federal Register to the extent that these regulations affect members of the public; (c) establish procedures to prevent unnecessary access to classified information, including procedures that (i) require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs; and (d) develop special contingency plans for the protection of classified information used in or near hostile or potentially hostile areas.

Sec. 5.4 Sanctions.

(a) If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior official designated under Section 5.3(a)(1) [FN1] so that corrective steps, if appropriate, may be taken. (b) Officers and employees of the United States Government, and its contractors, licensees, and grantees shall be subject to appropriate sanctions if they: (1) knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under this Order or predecessor orders; (2) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive; or (3) knowingly and willfully violate any other provision of this Order or implementing directive. (c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified

information, or other sanctions in accordance with applicable law and agency regulation. (d) Each agency head or the senior official designated under Section 5.3(a)(1) [FN1] shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5.4(b) occurs. Either shall ensure that the Director of the Information Security Oversight Office is promptly notified whenever a violation under Section 5.4(b)(1) or (2) occurs.

Part 6

General Provisions

Sec. 6.1 Definitions.

(a) 'Agency' has the meaning provided at 5 U.S.C. 552(e). (b) 'Information' means may information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. (c) 'National security information' means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated. (d) 'Foreign government information' means: (1) information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence. (e) 'National security' means the national defense or foreign relations of the United States. (f) 'Confidential source' means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence. (g) 'Original classification' means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

Sec. 6.2 General.

(a) Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended. 'Restricted Data' and 'Formerly Restricted Data' shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the

Atomic Energy Act of 1954, as amended, and regulations issued under that Act. (b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this Order with respect to any question arising in the course of its administration. (c) Nothing in this Order limits the protection afforded any information by other provisions of law. (d) Executive Order No. 12065 of June 28, 1978, as amended, is revoked as of the effective date of this Order. (e) This Order shall become effective on August 1, 1982.

I have taken the liberty of attaching hereto a Government guide relating to the handling of data spills.

The unauthorized publication of classified documents still receives little constitutional protection outside the context of prior restraint. The government can prosecute people for publishing or otherwise disseminating classified information, and classified documents are exempt from the requirements of the Freedom of Information Act. The Government has marked both of the charging documents in this case as "SECRET". This classification requires the removal of "SECRET" pursuant to a specific Government protocol you appear to be confusing with the unsealing of an Indictment. Equating same is incorrect and problematic. A sealed document, be it an Indictment or other pleading or document, does not mean the document is classified.

Classification of a document by marking same comes with it certain connotations.

To be clear, data spills, also known as data breaches or data leaks according to the National Initiative for Cybersecurity Careers and Studies, are the unauthorized movement or disclosure of classified or sensitive information to a party not authorized to possess or view the material. Unlike a hack, where an unauthorized user attempts to gain and maliciously use data, spills are usually the result of human error or carelessness. Until a document has been "unmarked" as classified per the Government protocol, the document cannot be leaked, spilled, or otherwise disseminated.

I have noted yet apparently you do not appreciate the impact of disclosure by the Government of Dr. Derges' personal identifying information ("PII").

The term "PII," refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual. Here you published the date of birth of Dr. Derges.

Sensitive PII includes, in addition to social security number:

- citizenship or immigration status,
- medical information,

- salary,
- ethnic or religious affiliation,
- personal email address, address, and phone
- account passwords,
- date of birth,
- criminal history, or
- mother's maiden name

I provide you with the foregoing out of an abundance of hope that you will see fit to immediately remediate fully the classification issue, spill issue, and re-visit the onerous, nay draconian, restrictions you attempt to impose on the Defense in this matter.

I will be addressing an out-of-town matter for the remainder of this week but will have access to my email.

Very truly yours,

Albert S. Watkins, LC
Watkins LLC, dba
Kodner Watkins
7733 Forsyth Blvd., Suite 600
St. Louis, MO 63105
Phone: 314-727-9111
Email: albertswatkins@kwklaw.net

From: Kempf, Shannon (USAMOW) [mailto:Shannon.Kempf@usdoj.gov]
Sent: Monday, March 29, 2021 11:12 AM
To: Albert Watkins <al@kwklaw.net>
Subject: RE: USA v. Derges [21-145][AG SF]

Dear Mr. Watkins:

The United States Attorney's Office requested that the indictment and the superseding indictment be filed under seal. In response, the Court sealed both documents and affixed the stamp at the top of both documents. Upon your client's first appearance on both the original indictment and the superseding indictment, I moved for the Court to unseal the documents, which the Court did.

If you have any further concerns in this regard, please bring the matter to the attention of the Court in a pretrial motion.

Sincerely,

Shannon Kempf
Assistant United States Attorney
Western District of Missouri

From: Albert Watkins <al@kwklaw.net>
Sent: Saturday, March 27, 2021 4:46 PM
To: Kempf, Shannon (USAMOW) <SKempf@usa.doj.gov>
Cc: Robert Seipp <rseipp@kwklaw.net>; Tony Bretz <tbretz@kwklaw.net>; Aimee Gronborg <agronborg@kwklaw.net>
Subject: USA v. Derges [21-145][AG SF]

Dear Mr. Kempf:

It was a pleasure meeting you on Friday in Court. Again, I apologize for misattribution of your given name to the incorrect gender.

I traveled back to St. Louis after the hearing and gave thought to the sensitivity and importance of the issue raised herein. As a result, I felt it prudent to issue this letter to you on a Saturday.

As a follow-up to the classification issue raised in Court Friday, I am concerned about the publication of the original Indictment in the above case on the internet with the classification stamp of "SECRET" in red bold type large print.

I was surprised to be handed in Court by you on Friday a copy of the Superseding Indictment with the similar classification mark "SECRET."

As shared with you, I have concern about the publication by the Government of classified material. I share this concern with you as an advocate for my client who is cast in a more unfavorable light by virtue of the marking. As also shared, I am concerned about the use of the "SECRET" stamp if the Indictment and the Superseding Indictment are not duly classified as "SECRET."

I have carefully reviewed the Indictment and the Superseding Indictment. Candidly, there does not appear to be anything in either the Indictment or the Superseding Indictment which would support the classification of either the Indictment or Superseding Indictment as "SECRET."

My review of both the Indictment and the Superseding Indictment gave rise to the clear noting of the absence of an end "SECRET" at both the top and the bottom of a classified document, a requirement under a long established and standing Government protocol.

The Indictment and Superseding Indictment herein are marked "SECRET" at the top but not at the bottom.

If a document is not duly classified, it is not lawful to mark same as such. Indeed, if the Indictment and Superseding Indictment are not truly classified, neither should have been marked as such in the first place.

If the Indictment and Superseding Indictment are truly classified such as to warrant being marked by the Government, please confirm with me that which specifically is contained in both the Indictment and Superseding Indictment which warranted the classified status.

If indeed the Indictment and Superseding were classified, the declassification of same must be approved and the classification mark, "SECRET", must be removed prior to release.

The Government has protocols and U.S. Code provisions which have been in place for as long as I can remember to address the "spill" of material marked as classified. Given what appeared to me to be an absence of familiarity by with you with that term of art, I wish to confirm that a "spill" is classified information appearing on unclassified computers, computers systems, and released to anyone without a secret classified clearance.

The release by the Government of the Indictment and Superseding Indictment as marked is wrong. Immediate measures need to be taken to report the spill and remediate same.

During our conversation yesterday in Court you indicated this was not something you were responsible for. As I noted, you are my contact with the Government in connection with this case. I am writing to you in your disclosed entry as the Assistant U.S. Attorney acting as counsel for the Government in this matter.

I am troubled by the first and second press releases of the Government in connection with this case. I am troubled by the press conference conducted by the Government contemporaneously with the announced of the initial Indictment herein. As part of this concern, in re-reviewing the Government's published iterations of the classified Indictment and Superseding Indictment, I noted the Government published for the world to see (on the internet) the classified Indictment without first removing personal identifying information of the Defendant. I request measures be taken immediately by the Government to remediate the foregoing.

Given the sensitivity of this for my client and the Government, I request immediate attention be given to this matter. Given our discussion yesterday and this correspondence, I consider my efforts to get this promptly addressed constitute a good faith effort to resolve this matter. However, if you wish to discuss same further over the weekend, please feel free to call me on my cell at 314-283-5736.

Very truly yours,

Albert S. Watkins, LC
Watkins LLC, dba
Kodner Watkins
7733 Forsyth Blvd., Suite 600
St. Louis, MO 63105
Phone: 314-727-9111
Email: albertswatkins@kwklaw.net